Attacco a La Poste, sottratti i dati di 22 milioni di persone e allarme truffe

Data: Invalid Date | Autore: Redazione



Nomi e indirizzi dei destinatari della corrispondenza aziendale coinvolti nella violazione di Maileva. Il caso richiama l’attenzione anche in Italia sulla sicurezza dei dati e sulle comunicazioni ingannevoli

Un **attacco informatico a Maileva**, società del **gruppo postale francese La Poste**, ha provocato il furto dei dati personali di circa **22 milioni di persone**. La violazione riguarda i destinatari delle comunicazioni inviate dalle aziende attraverso la piattaforma, utilizzata per gestire documenti e corrispondenza professionale.

L’intrusione risale alla **metà di settembre 2026**, mentre la conferma pubblica dell’entità del furto è arrivata il **14 novembre**. Le informazioni esposte comprendono **nomi, cognomi e indirizzi postali**. Secondo quanto comunicato dal gruppo, le coordinate bancarie non rientrano nei dati interessati.

Il rischio principale è che queste informazioni possano rendere più credibili tentativi di frode, attraverso comunicazioni personalizzate e richieste apparentemente attendibili.

Maileva e la gestione della corrispondenza aziendale

Maileva fa capo a **Docaposte**, la divisione digitale del gruppo La Poste. Offre servizi che consentono alle imprese di organizzare e spedire corrispondenza, dalle fatture alle raccomandate, fino alle buste paga e alle convocazioni delle assemblee.

La piattaforma dichiara oltre **70 mila utenti** e circa **180 milioni di documenti inviati nel 2024**. La sua posizione nella gestione delle comunicazioni spiega perché un singolo incidente possa coinvolgere un numero di persone molto superiore a quello delle aziende clienti.

Una persona può infatti ricevere una lettera elaborata tramite Maileva senza conoscere il servizio o avere un account sulla piattaforma. È questo passaggio, spesso poco visibile al destinatario, a rendere particolarmente rilevante la sicurezza dei fornitori esterni.

Quali dati sono stati rubati e cosa resta da chiarire

Le informazioni rese pubbliche indicano la sottrazione dei **dati identificativi e degli indirizzi postali** dei destinatari. L'utilizzo della piattaforma per spedire documenti professionali non significa, di per sé, che sia stato sottratto anche il contenuto di tutte le buste paga, fatture o raccomandate gestite dal servizio.

Maileva ha notificato l'incidente alla **Cnil**, l'autorità francese per la protezione dei dati personali, e ha presentato denuncia. Sull'accaduto è in corso un'**indagine giudiziaria**.

Occorre quindi distinguere le informazioni confermate dalle ipotesi sull'eventuale utilizzo successivo dei dati.

Perché nomi e indirizzi possono favorire le truffe

Anche senza password o coordinate bancarie, un archivio di **nomi e indirizzi**può essere sfruttato per costruire richieste ingannevoli. Una comunicazione che riporta dati corretti può apparire autentica e indurre il destinatario ad abbassare la guardia.

Tra gli scenari possibili ci sono false richieste di pagamento, avvisi di consegna e solleciti che imitano quelli di aziende o enti conosciuti. Se le informazioni vengono associate a recapiti telefonici o indirizzi email ottenuti altrove, possono inoltre facilitare campagne di **phishing** e **smishing**, le frodi realizzate rispettivamente tramite email e Sms.

Si tratta di possibili conseguenze di una violazione di questo tipo, non della conferma che tutti questi utilizzi siano già avvenuti nel caso Maileva.

Quali sono i rischi per gli utenti italiani

Le informazioni disponibili sul caso **non documentano un coinvolgimento di Poste Italiane o dei suoi sistemi**. La violazione riguarda Maileva e il gruppo francese La Poste: non consente quindi di concludere che siano stati sottratti dati dei titolari di conti o carte italiani.

L'attenzione per l'Italia riguarda soprattutto il meccanismo dell'attacco. Un fornitore che gestisce comunicazioni per numerose organizzazioni può concentrare grandi quantità di dati, diventando un bersaglio capace di esporre anche persone che non hanno rapporti diretti con lui.

Per gli utenti, la conseguenza pratica è chiara: **conoscere nome e indirizzo del destinatario non dimostra l'autenticità di un messaggio**. Anche una richiesta personalizzata deve essere verificata prima di effettuare pagamenti o comunicare informazioni riservate.

Come riconoscere una comunicazione sospetta

Un avviso di raccomandata, un pacco in giacenza o una fattura da saldare possono diventare il pretesto per indirizzare la vittima verso una pagina falsa. Meritano particolare attenzione i messaggi che impongono scadenze immediate, minacciano il blocco di un servizio o chiedono piccoli versamenti per completare una consegna.

Per verificare la richiesta è preferibile **aprire autonomamente l'app ufficiale**oppure digitare l'indirizzo del sito nel browser. In alternativa, si può contattare l'organizzazione attraverso un recapito già conosciuto, evitando quelli indicati nella comunicazione sospetta.

Password, Pin e codici temporanei di autorizzazionenon devono essere comunicati a chi li richiede tramite messaggi o telefonate. La presenza di un logo, di una firma o di dati anagrafici corretti non offre una garanzia sufficiente.

Cosa fare se sono stati comunicati dati o autorizzati pagamenti

Se una comunicazione sospetta ha portato a inserire credenziali su un sito, occorre cambiarle attraverso il servizio autentico e verificare gli accessi all'account. Quando la stessa password è utilizzata altrove, va sostituita anche sugli altri servizi.

Se sono stati forniti dati di pagamento o autorizzate operazioni, è necessario **contattare subito la banca o l'emittente della carta**, utilizzando i canali ufficiali, per valutare il blocco dello strumento e gli interventi possibili.

È utile conservare messaggi, ricevute e schermate da mettere a disposizione della **Polizia Postale**in caso di segnalazione o denuncia. Attivare l'**autenticazione a due fattori**e controllare regolarmente accessi e movimenti aiuta inoltre a individuare tempestivamente eventuali anomalie.

Articolo scaricato da www.infooggi.it
https://www.infooggi.it/articolo/attacco-a-la-poste-sottratti-i-dati-di-22-milioni-di-persone-e-allarme-truffe/158377